LIMITING THE OUTPUT OF ALERTS GENERATED BY AN INTRUSION DETECTION SENSOR DURING A DENIAL OF SERVICE ATTACK

ABSTRACT

An intrusion detection system is improved by altering its signatures and thresholds during a denial of service attack, in order to decrease the rate at which an intrusion detection sensor sends alerts to an intrusion detection server. A governor within the sensor is associated with each signature. The governor may include an alert log, a timer, an alert-generation-rate threshold, and rules that prescribe actions to be taken when the alert-generation-rate threshold is exceeded. The governor records the generation time of each alert by the sensor, and determines the rate at which the sensor is presently generating alerts. When the present alert-generation rate exceeds the alert-generation-rate threshold, the governor alters the associated signature threshold to decrease the alert generation rate of the intrusion detection sensor.